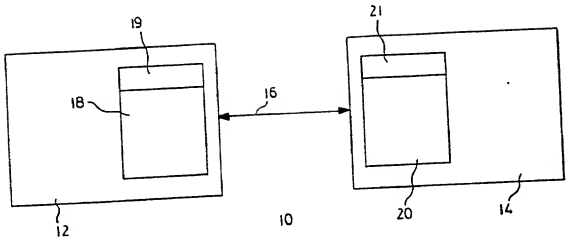

FIG. 1

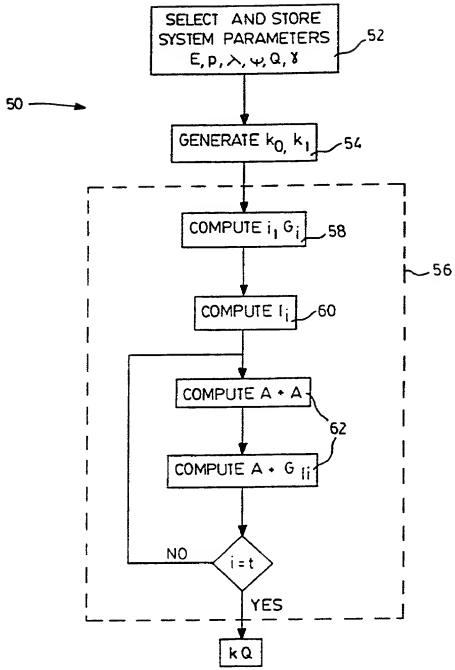
SELECT AND STORE
SYSTEM PARAMETERS
E, p, λ, ψ, Q, γ
52
50
GENERATE k_0, k_1
54
COMPUTE i_1 G_i
58
56
COMPUTE I_i
60
COMPUTE A + A
62
COMPUTE A + G_{Ii}
NO
i = t
YES
kQ

FIG. 2

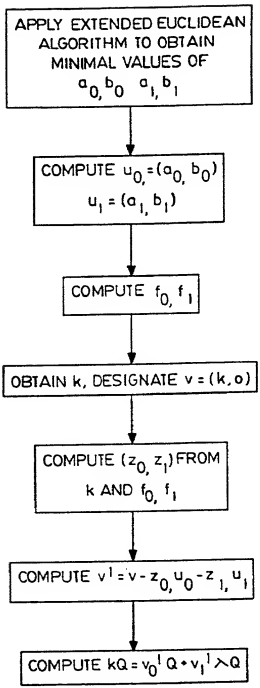
APPLY EXTENDED EUCLIDEAN ALGORITHM TO OBTAIN MINIMAL VALUES OF a_0, b_0 a_1, b_1
COMPUTE $u_0 = (a_0, b_0)$ $u_1 = (a_1, b_1)$
COMPUTE f_0, f_1
OBTAIN k, DESIGNATE $v = (k, o)$
COMPUTE (z_0, z_1) FROM k AND f_0, f_1
COMPUTE $v^1 = v - z_0, u_0 - z_1, u_1$
COMPUTE $kQ = v_0^1 Q + v_1^1 \wedge Q$

FIG. 3